#2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

EXPRESS MAIL NO. EL903022438US

Applicant	:	Hee-Jun Kim
Application No.	:	N/A
Filed	:	September 25, 2001
Title	:	METHOD FOR PREVENTING THEFT OF VEHICLE BY PERFORMING IGNITION KEY AUTHORIZATION
Grp./Div.	:	N/A
Examiner	:	N/A
Docket No.	:	47358/DBP/Y35

LETTER FORWARDING CERTIFIED PRIORITY DOCUMENT

Post Office Box 7068
Pasadena, CA 91109-7068
September 25, 2001

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Enclosed is a certified copy of Korean patent Application No. 2000-56124, which was filed on September 25, 2000, the priority of which is claimed in the above-identified application.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____
D. Bruce Prout
Reg. No. 20,958
626/795-9900

DBP/aam
Enclosure: Certified copy of patent application

AAM PAS382858.1-*-9/25/01 10:02 AM

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 56124 호
Application Number

출 원 년 월 일 : 2000년 09월 25일
Date of Application

출 원 인 : 현대자동차주식회사
Applicant(s)

CERTIFIED COPY OF PRIORITY DOCUMENT

2001 년 02 월 08 일

특 허 청
COMMISSIONER

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0009
【제출일자】 2000.09.25
【발명의 명칭】 시동키 인증을 통한 차량 도난 방지방법
【발명의 영문명칭】 A METHOD FOR PREVENTING THEFT OF VEHICLE THROUGH AUTHENTICATION OF IGNITION KEY

【출원인】
【명칭】 현대자동차주식회사
【출원인코드】 1-1998-004567-5

【대리인】
【성명】 오원석
【대리인코드】 9-1998-000474-3
【포괄위임등록번호】 1999-001089-4

【대리인】
【성명】 송만호
【대리인코드】 9-1998-000261-1
【포괄위임등록번호】 1999-001088-7

【발명자】
【성명의 국문표기】 김희준
【성명의 영문표기】 KIM,Hee Jun
【주민등록번호】 651223-1017512
【우편번호】 445-850
【주소】 경기도 화성군 남양면 장덕리 772-1
【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
오원석 (인) 대리인
송만호 (인)

【수수료】
【기본출원료】 20 면 29,000 원
【가산출원료】 6 면 6,000 원

【우선권주장료】	0 건	0	원
【심사청구료】	7 항	333,000	원
【합계】	368,000 원		
【첨부서류】	1. 요약서·명세서(도면)_1통		

【요약서】

【요약】

별도의 인증 장치 없이 엔진 제어수단에서 암호화 및 인증을 행하며, 다단계 비트 연산을 통해 무단 해독이 곤란하도록 구성된 시동키 인증을 통한 차량 도난 방지방법을 제공하기 위하여,

키 ID, 록 패스워드, 키 패스워드가 저장된 시동키 및 엔진 제어수단을 이용하여 시동키 인증을 통한 차량 도난 방지하는 방법에 있어서

(1) ECU가 시동키로부터 키 ID를 입력받고 등록 ID인가 판단하는 단계;

(2) 등록 ID 인 경우에 난수를 발생시키고 상기 난수를 이용하여 저장된 록 패스워드를 암호화하고, 상기 난수 및 암호화된 록 패스워드를 상기 시동키의 트랜스폰더에 전송하는 단계;

(3) 트랜스폰더는 전송받은 상기 난수 및 암호화된 록 패스워드를 이용하여 록 패스워드를 암호 해독한 후 상기 해독된 록 패스워드가 저장된 록 패스워드인가 판단하는 단계;

(4) 트랜스폰더는 저장된 키 패스워드를 이용하여 키 패스워드를 암호화한 후 상기 암호화된 키 패스워드를 상기 ECU로 전송하는 단계;

(5) 상기 암호화된 키 패스워드를 전송받은 상기 ECU는 전송받은 상기 암호화된 키 패스워드를 해독하여 키 패스워드를 생성한 후 저장된 키 패스워드인가 판단하는 단계;

(6) 저장된 키 패스워드 인 경우에는 시동 록 상태를 해제하는 단계;

를 포함하는 시동키 인증을 통한 차량 도난 방지방법을 제공한다.

【대표도】

도 2

【색인어】

시동키, 인증, 도난 방지, 난수, 비트 연산

【명세서】

【발명의 명칭】

시동키 인증을 통한 차량 도난 방지방법{A METHOD FOR PREVENTING THEFT OF VEHICLE THROUGH AUTHENTICATION OF IGNITION KEY}

【도면의 간단한 설명】

도 1은 본 발명의 일 실시예에 의한 시동키 인증을 통한 차량 도난 방지방법이 수행되는 시동키 인증 시스템의 구성도이다.

도 2는 본 발명의 실시예에 의한 시동키 인증을 통한 차량 도난 방지방법을 나타낸 흐름도이다.

도 3은 상기 시프트 레지스터 T 및 S의 초기화 및 변조 과정을 나타낸 개념도이다.

도 4는 시프트 레지스터 T 및 S의 변조 과정을 나타낸 흐름도이다.

도 5는 1차 세션키를 생성하는 과정을 나타낸 개념도이다.

도 6은 1차 세션 키를 생성하는 과정을 나타낸 흐름도이다.

도 7은 SO 계산단계에서 수행되는 OUTPUT(i) 생성 과정을 나타낸 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<8> 본 발명은 시동키 인증을 통한 차량 도난 방지방법에 관한 것으로, 더욱 상세하게는, 별도의 인증 장치 없이 엔진 제어수단에서 암호화 및 인증을 행하는 방법에 관한 것이다.

<9> 주지하는 바와 같이, 차량이 위치 이동의 대표적인 수단으로 부각되면서 차량의 수요가 늘었고, 이에 따라 차량의 도난 또한 늘게 되었다.

<10> 따라서, 자동차 메이커에서는 차량의 도난 방지를 위해 각종 방법을 강구하고 있으며, 이 중에서 최근 획기적인 것으로 주목받고 있는 것은 시동키에 소정의 암호를 색인하고, 엔진이 상기 암호를 인식함으로써 최초 출고된 때 설정된 시동키 만으로 시동을 걸 수 있도록 하는 시동키 인증을 통한 차량 도난 방지방법이다.

<11> 그런데, 종래의 시동키 인증 방법은, 시동키에 설정된 암호(또는 식별번호)가 색인된 IC(Integrated Circuit)를 부착하고, 상기 IC의 암호(또는 식별번호)를 엔진 제어수단이 인식함으로써 인증하는 것이 대표적인 방법이었으며, 상기 IC 암호의 해독을 위해서는 별도의 암호 인증 장치를 부착하여, 상기 엔진 제어수단은 상기 암호 인증 장치로부터 출력되는 인증 신호를 기초로 엔진 시동을 허용할 것인가 여부를 판단하도록 한 것이다.

<12> 그런데 이 경우 별도의 시스템을 구비하여야 하므로 부품수를 증가시키고, 또한 엔진 제어수단과는 별도의 인증 장치에서 인증하여 인증 신호를 엔진 제어수단과 송수신함으로써, 외부에서 상기 송수신되는 신호를 검출하는 경우 정보 누출이 가능할 수 있다.

<13> 또한 종래의 암호화 방법은 인크립션(encryption) 또는 픽스코드(fixed code) 법이 있으나, 자동차용 키의 인증 방법으로는 픽스코드 법이 주로 사용되었으며, 이는 픽스코드가 부여된 키가 키박스에 투입될 때 상기 키로부터 픽스코드를 읽어 이가 등록된 여부를 별도의 인증 장치에서 판단하고, 엔진 제어수단은 상기 인증 장치로부터 판단 결과를 입력받아 엔진 시동 여부를 판단하는 방법에 의한 것이다.

【발명이 이루고자 하는 기술적 과제】

<14> 따라서, 본 발명의 목적은 별도의 인증 장치 없이 엔진 제어수단에서 암호화 및 인증을 행하며, 다단계 비트 연산을 통해 무단 해독이 곤란하도록 구성된 시동키 인증을 통한 차량 도난 방지방법을 제공하는 것이다.

【발명의 구성 및 작용】

<15> 상기 목적을 달성하기 위하여 본 발명에 의한 시동키 인증을 통한 차량 도난 방지방법은,

<16> 키 ID, 록 패스워드, 키 패스워드가 저장된 시동키 및 엔진 제어수단을 이용하여 시동키 인증을 통한 차량 도난 방지하는 방법에 있어서

<17> (1) ECU가 시동키로부터 키 ID를 입력받고 등록 ID인가 판단하는 단계;

<18> (2) 등록 ID 인 경우에 난수를 발생시키고 상기 난수를 이용하여 저장된 록 패스워드를 암호화하고, 상기 난수 및 암호화된 록 패스워드를 상기 시동키의 트랜스폰더에 전송하는 단계;

<19> (3) 트랜스폰더는 전송받은 상기 난수 및 암호화된 록 패스워드를 이용하여 록 패스워드를 암호 해독한 후 상기 해독된 록 패스워드가 저장된 록 패스워드인가 판단하는 단계;

<20> (4) 트랜스폰더는 저장된 키 패스워드를 이용하여 키 패스워드를 암호화한 후 상기 암호화된 키 패스워드를 상기 ECU로 전송하는 단계;

<21> (5) 상기 암호화된 키 패스워드를 전송받은 상기 ECU는 전송받은 상기 암호화된 키 패스워드를 해독하여 키 패스워드를 생성한 후 저장된 키 패스워드인가 판단하는 단계;

<22> (6) 저장된 키 패스워드 인 경우에는 시동 록 상태를 해제하는 단계;

<23> 를 포함하는 것을 특징으로 한다.

<24> 이하, 본 발명의 일 실시예를 첨부된 도면의 의거하여 상세히 설명하면 다음과 같다.

<25> 도 1은 본 발명의 일 실시예에 의한 시동키 인증을 통한 차량 도난 방지방법이 수행되는 시동키 인증 시스템의 구성도이다.

<26> 입력 암호를 해독하고, 암호를 연산하며, 연산된 신호를 암호화하는 트랜스폰더(transponder; 110)가 부착된 키(key; 120);

<27> 상기 키(key)가 끼워지며 상기 키(key)와 신호를 송수신하는 키 박스(key box; 130);

<28> 상기 키 박스를 통해 암호 신호를 송수신하는 엔진 제어수단(150)을 포함한다.

<29> 상기 키박스 내에는 코일 안테나(140)가 설치되어 상기 코일 안테나(140)를 통하여 상기 트랜스폰더(110)와 데이터를 송수신하며, 상기 엔진 제어수단(150)은 상기 코일 안테나(140)에 데이터 인터페이스(160)를 통해 연결되어 데이터를 송수신한다.

<30> 상기 키(key)의 트랜스폰더(110)는 암호화 및 암호의 해독, 연산을 할 수 있는 IC 칩으로 구성되며, 상기 엔진 제어수단(150)은 엔진을 제어하는 통상의 전자제어유닛(ECU)으로 한다.

<31> 상기 트랜스폰더(110) 내에는 제작 당시에 부여된 키 식별자(key identifier; 이하 'ID'라 칭한다)가 4 바이트(byte)로 설정되어 저장되며(1byte=8bit), 암호 인증을 위하여 인증 식별자(Authenticator; 이하 'AUTHEN'라 칭한다)가 6 바이트로 설정되어 저장되며, 4 바이트의 록 패스워드(Lock Password) 및 키 패스워드(key Password)가 설정되어 저장된다.

<32> 상기 엔진 제어수단(150) 내에는 암호화 및 암호의 해독, 연산을 위한 시프트 레지스터 T 및 S가 구비되며, 상기 트랜스폰더(110)에 저장된 키 ID, 인증 식별자(AUTHEN), 록 패스워드 및 키 패스워드와 동일한 키 ID, 인증 식별자(AUTHEN), 록 패스워드 및 키 패스워드가 저장된다.

<33> 도 2는 본 발명의 실시예에 의한 시동키 인증을 통한 차량 도난 방지방법을 나타낸 흐름도이다.

<34> 먼저, 시동키(120)가 키박스(130)에 투입되면, 상기 엔진 제어수단(150)은 상기 키(120)에 부착된 트랜스폰더(110)로부터 키 ID를 입력받는다(S210).

<35> 키 ID를 입력받은 엔진 제어수단(150)은 상기 키 ID가 등록된 ID인지 판단하고(S215), 등록된 ID가 아닌 경우에는 시동 록 상태(시동이 걸리지 않는 상태)를 유지한다(S217). 상기 시동 록 상태는 연료 공급 및 점화계통의 출력을 금지함으로써 할 수 있다.

<36> 등록된 ID인 경우에는 4 바이트 난수(random number; 이하 'RN'이라 칭한다)를 발생시킨다(S220).

<37> 난수를 발생시킨 후에는, 상기 입력된 키 ID 및 저장된 AUTHEN을 기초로 상기 시프트 레지스터 T 및 S를 초기화 및 변조한다(S225).

<38> 시프트 레지스터 T 및 S의 변조는, 상기 시프트 레지스터 T 및 S를 초기화한 후에는, 상기 입력된 키 ID, 저장된 AUTHEN, 및 상기 난수(RN)를 기초로 상기 시프트 레지스터 T 및 S를 변조하는 것이다.

<39> 도 3은 상기 시프트 레지스터 T 및 S의 초기화 및 변조 과정을 나타낸 개념도이다.

<40> 상기 시프트 레지스터 T 및 S는 도 3에 도시된 바와 같이, 최대중요비트(Most

Significant Bit; 이하 'MSB'라 칭한다)로부터 최소중요비트(Least Significant Bit; 이하 'LSB'라 칭한다)로 배열되며, 시프트 레지스터 T의 LSB와 시프트 레지스터 S의 MSB는 인접하게 배열된다.

<41> 상기 시프트 레지스터 T는 상기 트랜스폰더로부터 입력받은 키 ID(ID0, ID1, ID2 및 ID3의 4 바이트)의 ID0 및 ID1 바이트가 지정되며, 상기 시프트 레지스터 S는 상기 키 ID의 ID2, ID3 및 상기 저장된 AUTHEN(AUTHEN0 내지 AUTHEN 5의 6 바이트)의 AUTHEN 4, AUTHEN 5의 4 바이트가 순차적으로 지정된다.

<42> 상기 시프트 레지스터 S의 각 비트는 LSB로부터 MSB까지 S0 내지 S31까지 인덱싱되며, 시프트 레지스터 T의 각 비트는 LSB로부터 MSB까지 T0 내지 T15까지 인덱싱된다.

<43> 상기와 같이 시프트 레지스터 T 및 S를 초기화 한 후에는, 설정된 함수 F0, F1 및 F2를 이용하여 시프트 레지스터 S의 LSB를 계산하고, 상기 시프트 레지스터 T 및 S를 시프트 연산하는 과정을 반복함으로써 상기 시프트 레지스터 T 및 S를 변조한다.

<44> 상기 F0 및 F1 함수는 4개의 비트를 입력값으로 하여 하나의 비트를 연산하는 함수이며, F2 함수는 5개의 비트를 입력값으로 하여 하나의 비트를 연산하는 함수로서, 구체적으로는 아래와 같이 함수값을 계산한다.

<45> $$F0(a,b,c,d) = \overline{(a\times b\times \bar{d})+(a\times \bar{c}\times \bar{d})+(b\times c\times d)+(\bar{b}\times \bar{c}\times d)+(\bar{a}\times \bar{b}\times \bar{c}\times \bar{d})}$$

<46> $$F1(a,b,c,d) = \overline{(c\times d)+(\bar{a}\times \bar{b}\times c)+(\bar{a}\times \bar{b}\times d)+(a\times \bar{c}\times \bar{d})}$$

<47> $$F2(a,b,c,d,e)$$

$$= \overline{(c\times d\times e)+(\bar{a}\times b\times \bar{e})+(a\times \bar{b}\times c)+(b\times \bar{c}\times \bar{d}\times e)+(a\times \bar{b}\times d\times e)+(\bar{a}\times \bar{c}\times d\times \bar{e})+(a\times b\times \bar{c}\times d\times \bar{e})}$$

<48> 그런데 상기 F2의 입력값으로 사용되는 5 비트는 상기 시프트 레지스터 T 및 S로부터 연산된 값을 사용한다.

<49> 즉 F2 함수의 입력값을 (Q0,Q1,Q2,Q3,Q4)라고 할 때, Q0=F0(S1,S3,S4,S13), Q1=F1(S14,S16,S18,S19), Q2=F1(S21,S24,S26,S30), Q3=F1(T0,T1,T3,T7), 및 Q4=F0(T9,T10,T12,T13)으로 계산된 값이 입력되어 계산된다.

<50> 그런데, 상기 AUTHEN 은 AUTHEN0 내지 AUTHEN3 까지의 4바이트(즉, 32비트)의 각 비트는 AUTHEN(i)로 인덱싱되고, 상기 난수(RN)의 각 비트는 RN(i)로 인덱싱된다.

<51> 상기 F2 연산 결과에 따른 비트는, 상기 AUTHEN(i) 및 RN(i)와 조합되어 연산됨을 반복함으로써 상기 시프트 레지스터 T 및 S를 변조한다.

<52> 즉, 시프트 레지스터 T 및 S의 변조는 도 4와 같은 순서도에 의해 이루어진다.

<53> 먼저, 변수 i에 0을 대입하고(S410), 상기와 같이 F2 연산을 수행한다(S420).

<54> 시프트 레지스터 T를 1 비트 좌측으로 시프트한 후(S430), T0에는 S31의 값을 대입하고(S440), 시프트 레지스터 S를 1비트 좌측으로 시프트 한다(S450).

<55> S0에는 상기 RN(i)와 AUTHEN(i) 및 F2 연산 결과값을 XOR 연산한 값을 지정한다(S460). 즉, 'S0 = RN(i)??AUTHEN(i)??F2연산 결과값'과 같이 연산된다. 상기 '??' 연산은 XOR 즉, 연산자의 좌우측에 있는 값이 서로 다를 경우에 1을, 같은 경우에는 0을 출력하는 연산자이다.

<56> 상기(S420~S460)와 같이 시프트 레지스터 T 및 S를 1회 시프트 연산한 후에는, 상기 변

수 i 가 31이 되었는지 판단하고(S470), 31이 되지 않은 경우에는 상기 변수 i에 1을 더하여(S480) 상기 F2연산단계(S420)로 진행함으로써, 상기 시프트 레지스터 T 및 S를 총 32회 시프트 연산하게 된다.

<57> 다시 도 2를 참조로, 시프트 레지스터 T 및 S를 초기화 및 변조한 후에는 상기 변조된 시프트 레지스터 T 및 S, 그리고 설정된 인터널 키(internal key)를 이용하여 1차 세션 키(cession key)를 생성한다(S230).

<58> 상기 인터널 키(internal key)는 6 바이트 숫자로 설정된다.

<59> 도 5는 상기 1차 세션키를 생성하는 과정을 나타낸 개념도이다.

<60> 초기화된 상기 시프트 레지스터 T 및 S는 도 5에 도시된 바와 같이, MSB로부터 LSB로 배열되며, 시프트 레지스터 T의 LSB와 시프트 레지스터 S의 MSB는 인접하게 배열된다.

<61> 상기 인터널 키는 도 5에 도시된 바와 같이, 상기 시프트 레지스터 T 및 S와 비트끼리 대응하도록 배열된다.

<62> 1차 세션 키를 생성하기 위해 시프트 레지스터로부터 비트 연산하는 F0, F1, F2 함수가 정의되며, 상기 F0, F1,F2 함수는 시프트 레지스터 초기화에 사용된 동일한 함수로 정의된다.

<63> 상기 F2 함수에 의해 1차 세션 키의 각 비트가 연산되게 되며, 1차 세션 키의 하나의 비트가 연산된 후에는 상기 시프트 레지스터 T 및 S의 좌측 시프트 연산하고, 도 5의 A와 같이 특별히 정의된 연산에 의해 S0 비트를 결정한다.

<64> 이러한 과정을 반복함으로써 1차 세션 키를 계산하게 되는 것이다.

<65> 도 6은 상기 1차 세션 키를 생성하는 과정을 나타낸 흐름도이다.

<66> 먼저, 변수 i 에 0을 대입하고, Result 변수에 0을 대입함으로써 변수를 초기화한다 (S610),

<67> 변수를 초기화 한 후에는 상기와 같이 정의된 F2 연산을 수행함으로써 1차 세션 키의 i 번째 비트 값을 구한다(S620).

<68> 시프트 레지스터 T를 1 비트 좌측으로 시프트한 후(S630), T0에는 S31의 값을 대입하고 (S640), 시프트 레지스터 S를 1비트 좌측으로 시프트 한다(S650).

<69> S0에는 설정된 OUTPUT 함수에 의해 OUTPUT(i)를 생성하여 S0에 대입한다(S660).

<70> 상기(S620~S660)와 같이 시프트 레지스터 T 및 S를 1회 시프트 연산한 후에는, 상기 변수 i 가 31이 되었는지 판단하고(S670), 31이 되지 않은 경우에는 상기 변수 i에 1을 더하여(S680) 상기 F2연산단계(S620)로 진행함으로써, 상기 시프트 레지스터 T 및 S를 총 32회 시프트 연산하게 된다.

<71> 도 7은 상기 S0 계산단계(S660)에서 수행되는 OUTPUT(i) 생성 과정을 나타낸 흐름도이다.

<72> 먼저 변수 j에 0을 대입한다(S710).

<73> 인터널 키의 j 번째 비트(Pj)가 1인지 판단한다(S720).

<74> 상기 판단(S720)에서 1인 경우에, j가 31 이하인지 판단하여(S730), j가 31 이하인 경우에는 Sj(레지스터 S의 j번째 비트)를, j가 31을 초과하는 경우에는 Tj-32(레지스터 T의 j-32 번째 비트)를 변수 Result 와 XOR 연산하여 변수 Result에 대입한다 (SS740,S750).

<75> 상기 판단(S720)에서 1이 아니거나, 상기(S740,S750)와 같이 Result 값을 갱신한 후에

는, j가 47인지 판단하여(S760), 47이 아닌 경우에는 상기 Pj 판단단계(S720)로 진행하여 상기 인터널 키의 모든 비트에 대하여 연산할 수 있도록 한다.

<76> 상기 j 판단단계(S760)에서 47인 경우에는 OUTPUT(i) 값을 계산된 Result 값으로 결정한다(S770).

<77> 상기와 같이 OUTPUT(i) 값을 결정한 후에는 상기 SO 계산단계(S660)는 종료한다.

<78> 도 2에 도시된 바와 같이, 1차 세션 키를 생성한 후에는, 록 패스워드 암호화 연산을 수행한다(S235).

<79> 상기 록 패스워드 암호화 연산은 저장된 록 패스워드 및 상기 1차 세션 키를 이용하여 암호화하며, 각각 4 바이트로 형성된 상기 록 패스워드 및 상기 1차 세션 키를 XOR 연산하는 것이다.

<80> 록 패스워드 암호화 연산을 수행한 후에는 상기 엔진 제어수단(150)은, 상기 난수 및 암호화된 록 패스워드를 상기 트랜스폰더(110)에 전송하고(S240), 상기 트랜스폰더(110)는 상기 난수 및 암호화된 록 패스워드를 수신한다(S242).

<81> 상기 트랜스폰더(110)는 상기 엔진 제어수단이 1차 세션 키를 생성한 과정(S225,S230)과 동일한 과정에 의해 1차 세션 키를 생성한다(S245).

<82> 상기 동일한 과정은 1차 세션 키를 생성하는 동일한 논리에 의해 생성되는 것으로써, 상기 트랜스폰더(110) 내에 시프트 레지스터를 구비하지 아니하여도 회로 구성에 의하여 상기 논리대로 생성되도록 하는 것이 바람직하다.

<83> 따라서 상기 트랜스폰더(110)에 의해 생성된 1차 세션 키는 상기 엔진 제어수단(150)에 의해 생성된 1차 세션 키와 같게 된다.

<84> 1차 세션 키를 생성한 상기 트랜스폰더는 상기 1차 세션 키와 암호화된 록 패스워드를 XOR 연산함으로써 록 패스워드를 해독한다(S250).

<85> 즉, 동일한 1차 세션 키를 이용하여 XOR 연산을 거듭 수행함으로써 암호화 및 해독이 가능한 것이다.

<86> 록 패스워드를 해독한 상기 트랜스폰더(110)는 해독된 록 패스워드가 저장된 록 패스워드와 동일한지 판단하고(S255), 동일하지 않은 경우에는 본 발명의 실시예의 시동키 인증방법은 종료되어 시동 록 상태가 유지된다.

<87> 상기 록 패스워드 판단단계(S255)에서 동일한 경우에는 변조된 시프트 레지스터 T 및 S 값을 기초로 상기 1차 세션 키를 생성한 과정(S230)과 동일한 과정에 의해 2차 세션 키를 생성한다(S260).

<88> 2차 세션 키를 생성한 트랜스폰더(110)는 저장된 키 패스워드와 상기 생성된 2차 세션 키를 XOR 연산함으로써 키 패스워드를 암호화한다(S265).

<89> 키 패스워드를 암호화한 후에는 상기 암호화된 키 패스워드를 엔진 제어수단(150)으로 전송하고(S270), 엔진 제어수단(150)은 상기 암호화된 키 패스워드를 수신한다(S272).

<90> 키 패스워드를 수신한 엔진 제어수단(150)은 상기 1차 세션 키를 생성한 과정(S230)과 동일한 과정에 의해 변조된 시프트 레지스터 T 및 S 값을 기초로 2차 세션 키를 생성한다(S275).

<91> 2차 세션 키를 생성한 엔진 제어수단(150)은 상기 생성된 2차 세션 키와 수신된 암호화 키 패스워드를 XOR 연산함으로써 키 패스워드를 해독한다(S280).

<92> 키 패스워드를 해독한 상기 엔진 제어수단(150)은 해독된 키 패스워드가 저장된 키 패

스워드와 동일한지 판단하고(S285), 동일하지 않은 경우에는 시동 록 상태(시동이 걸리지 않는 상태)를 유지한다(S287).

<93> 해독된 키 패스워드가 저장된 키 패스워드와 동일한 경우에는 시동 록 상태를 해제한다(S290). 상기 시동 록 상태의 해제는 연료공급 및 점화계통의 출력을 허용함으로써 할 수 있다.

<94> 이상으로 본 발명의 시동키 인증을 통한 차량 도난 방지방법에 관한 바람직한 실시예를 설명하였으나, 본 발명은 상기 실시예에 한정되지 아니하며, 본 발명의 실시예로부터 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의한 용이하게 변경되어 균등하다고 인정되는 범위의 모든 변경을 포함한다.

【발명의 효과】

<95> 본 발명의 실시예에 의하면, 각종 패스워드의 암호화 및 해독을 엔진 제어수단 내에서 수행함으로써, 보안성이 향상된다.

<96> 또한 비트 연산을 다단계로 행하여 암호화 및 해독함으로써 암호의 신뢰성이 높일 수 있다.

<97> 그리고, 시동키 인증을 위한 별도의 부가장치를 구비하지 않아도 되므로 공정 및 생산비용을 줄일 수 있으며, 별도 부가장치에 낭비되는 공간을 줄일 수 있다.

【특허청구범위】

【청구항 1】

키 ID, 록 패스워드, 키 패스워드가 저장된 시동키 및 엔진 제어수단을 이용하여 시동키 인증을 통한 차량 도난 방지하는 방법에 있어서

(1) ECU 가 시동키로부터 키 ID를 입력받고 등록 ID인가 판단하는 단계;

(2) 등록 ID 인 경우에 난수를 발생시키고 상기 난수를 이용하여 저장된 록 패스워드를 암호화하고, 상기 난수 및 암호화된 록 패스워드를 상기 시동키의 트랜스폰더에 전송하는 단계;

(3) 트랜스폰더는 전송받은 상기 난수 및 암호화된 록 패스워드를 이용하여 록 패스워드를 암호 해독한 후 상기 해독된 록 패스워드가 저장된 록 패스워드인가 판단하는 단계;

(4) 트랜스폰더는 저장된 키 패스워드를 이용하여 키 패스워드를 암호화한 후 상기 암호화된 키 패스워드를 상기 ECU로 전송하는 단계;

(5) 상기 암호화된 키 패스워드를 전송받은 상기 ECU는 전송받은 상기 암호화된 키 패스워드를 해독하여 키 패스워드를 생성한 후 저장된 키 패스워드인가 판단하는 단계;

(6) 저장된 키 패스워드 인 경우에는 시동 록 상태를 해제하는 단계;

를 포함하는 시동키 인증을 통한 차량 도난 방지방법.

【청구항 2】

제1항에서,

ECU는 시프트 레지스터 T 및 S를 포함하고,

상기(2)단계에서, 저장된 록 패스워드의 암호화는,

(7) 상기 난수를 이용하여 상기 시프트 레지스터 T 및 S를 초기화 및 변조하는 단계;

(8) 1 차 세션 키를 생성하는 단계;

(9) 상기 1차 세션 키를 이용하여 저장된 록 패스워드를 암호화하는 단계;

를 포함하고,

상기(3)단계에서, 상기 난수 및 암호화된 록 패스워드를 이용하여 록 패스워드를 해독하는 것은, 상기(2)단계에서 상기 난수를 이용하여 저장된 록 패스워드를 암호화하는 것과 동일한 방법에 의해 해독되는 것을 특징으로 하는 시동키 인증을 통한 차량 도난 방지방법.

【청구항 3】

제2항에서,

상기(7)단계의 시프트 레지스터 초기화는 난수를 발생하는 단계를 포함하고,

상기(7)단계의 시프트 레지스터 변조는,

복수개의 비트 값을 입력받아 하나의 비트값을 연산하는 복수개의 함수가 정의되고, 상기 정의된 복수개의 함수로부터 연산 결과값을 입력받아 비트값을 연산하는 F2함수가 정의되어,

상기 시프트 레지스터 T 및 S를 시프트 레프트 하는 연산 및 상기 F2 함수값과 상기 난수의 하나의 비트를 이용하여 상기 시프트 레지스터 S의 LSB를 결정하는 과정을 복수번 반복함으로써 이루어지는 것을 특징으로 하는 시동키 인증을 통한 차량 도난 방지방법.

【청구항 4】

제2항에서,

상기(8)단계의 1차 세션 키 생성은

복수개의 비트값을 입력받아 하나의 비트값을 연산하는 복수개의 함수가 정의되고, 상기 정의된 복수개의 함수로부터 연산 결과값을 입력받아 비트값을 연산하는 F3함수가 정의되어,

상기 F3 함수값으로써 상기 1차 세션 키의 비트를 연산하는 것을 특징으로 하는 시동키 인증을 통한 차량 도난 방지방법.

【청구항 5】

제4항에서,

상기 복수개의 함수는 상기(7)단계의 복수개의 함수와 동일하며, 상기 F3 함수는 상기 F2 함수와 동일한 것을 특징으로 하는 시동키 인증을 통한 차량 도난 방지방법.

【청구항 6】

제1항에서,

ECU 는 시프트 레지스터 T 및 S를 포함하고,

상기(4)단계에서, 저장된 키 패스워드의 암호화는,

(10) 2 차 세션 키를 생성하는 단계;

(11) 상기 2차 세션 키를 이용하여 저장된 키 패스워드를 암호화하는 단계;

를 포함하고,

상기(5)단계에서, 암호화된 키 패스워드 해독은, 상기(4)단계에서 키 패스워드를 암호

화하는 것과 동일한 방법에 의해 해독되는 것을 특징으로 하는 시동키 인증을 통한 차량 도난 방지방법.

【청구항 7】

제6항에서,

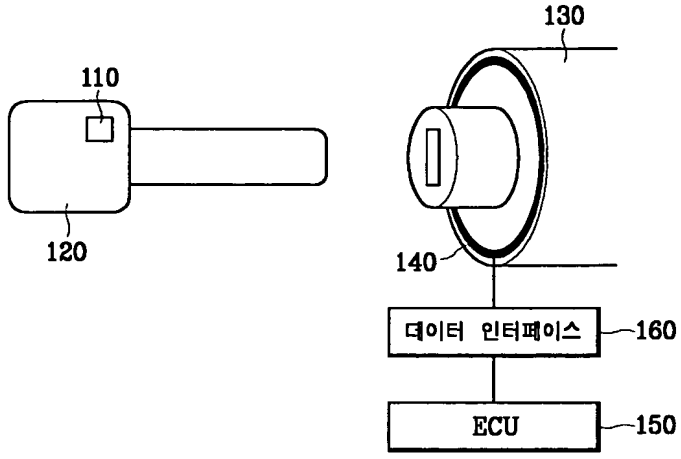
상기(10)단계의 2차 세션 키 생성은

복수개의 비트값을 입력받아 하나의 비트값을 연산하는 복수개의 함수가 정의되고, 상기 정의된 복수개의 함수로부터 연산 결과값을 입력받아 비트값을 연산하는 F4함수가 정의되어,

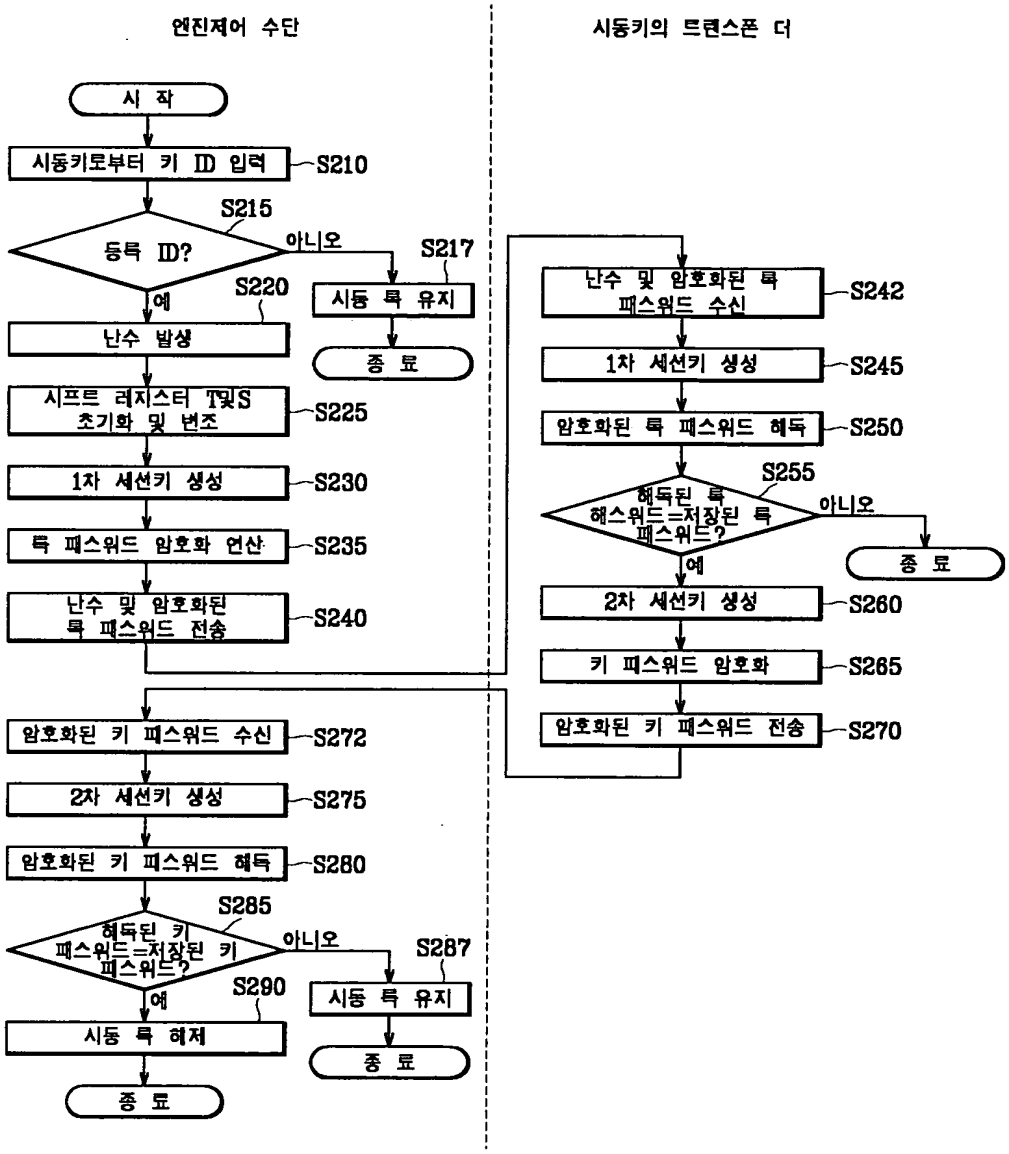
상기 F4 함수값으로써 상기 1차 세션 키의 비트를 연산하는 것을 특징으로 하는 시동키 인증을 통한 차량 도난 방지방법.

【도면】

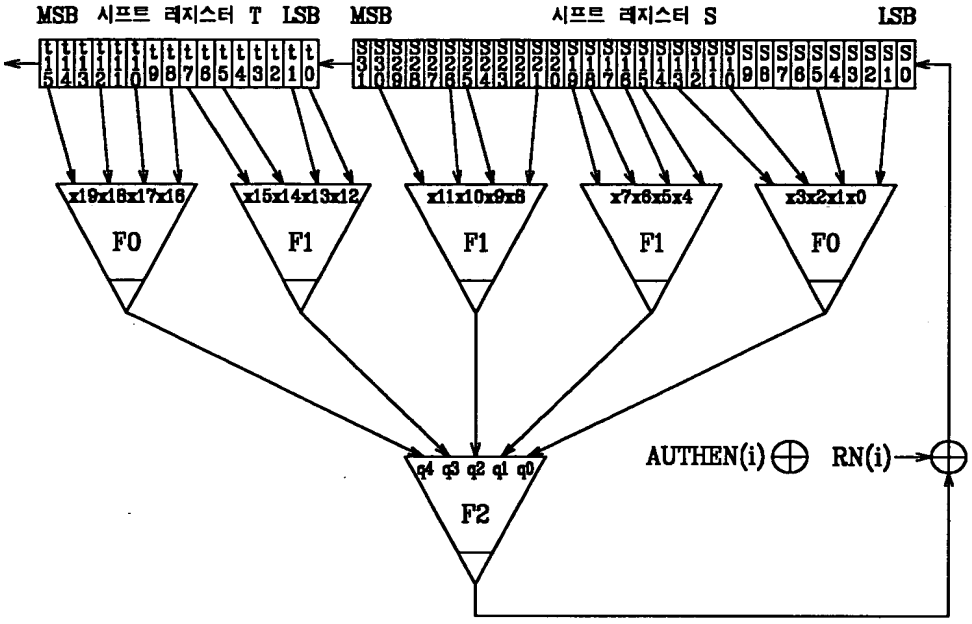
【도 1】



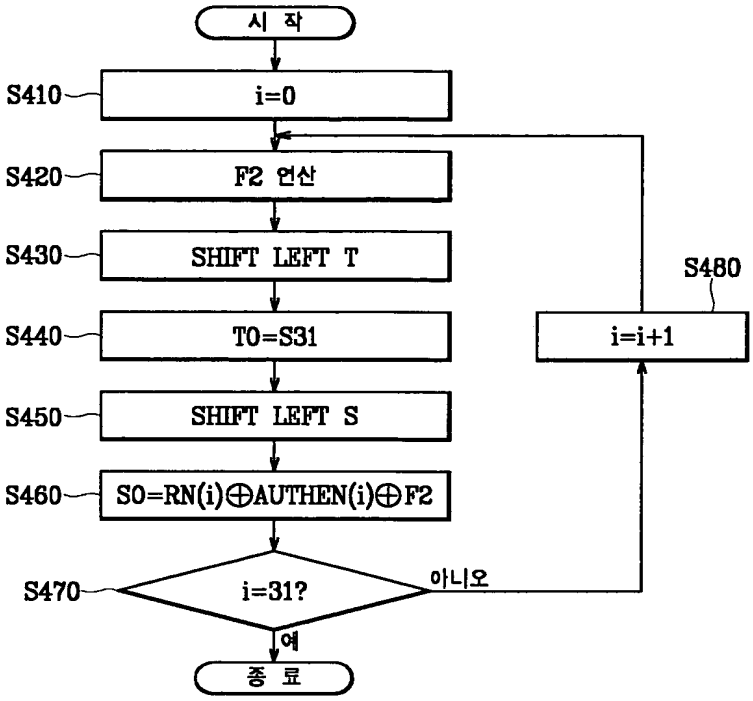
【도 2】


엔진제어 수단
시동키의 트랜스폰 더
시 작
시동키로부터 키 ID 입력
S210
S215
등록 ID?
아니오
S217
시동 록 유지
종 료
예
S220
난수 발생
시프트 레지스터 T및S 초기화 및 변조
S225
1차 세션키 생성
S230
록 패스워드 암호화 연산
S235
난수 및 암호화된 록 패스워드 전송
S240
난수 및 암호화된 록 패스워드 수신
S242
1차 세션키 생성
S245
암호화된 록 패스워드 해독
S250
S255
해독된 록 해스워드=저장된 록 패스워드?
아니오
종 료
예
2차 세션키 생성
S260
키 패스워드 암호화
S265
암호화된 키 패스워드 전송
S270
암호화된 키 패스워드 수신
S272
2차 세션키 생성
S275
암호화된 키 패스워드 해독
S280
S285
해독된 키 패스워드=저장된 키 패스워드?
아니오
S287
시동 록 유지
종 료
예
S290
시동 록 해제
종 료

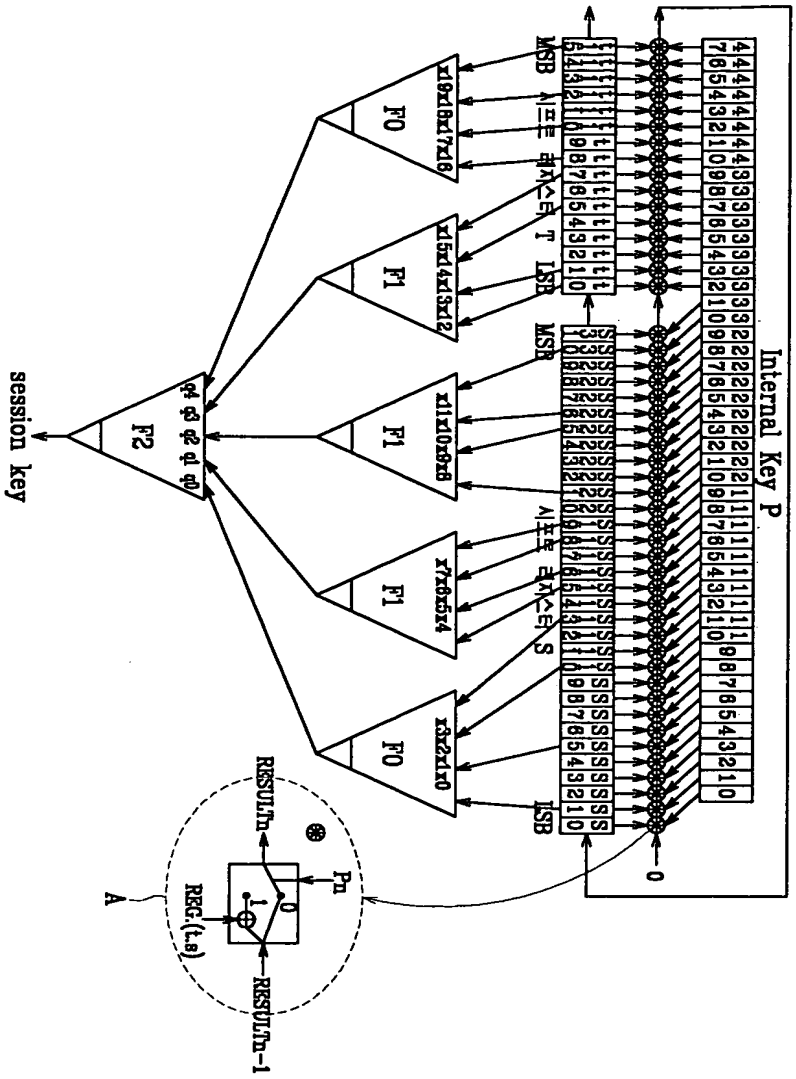
【도 3】


MSB
시프트 레지스터 T
LSB
MSB
시프트 레지스터 S
LSB
t15 t14 t13 t12 t11 t10 t9 t8 t7 t6 t5 t4 t3 t2 t1 t0
S31 S30 S29 S28 S27 S26 S25 S24 S23 S22 S21 S20 S19 S18 S17 S16 S15 S14 S13 S12 S11 S10 S9 S8 S7 S6 S5 S4 S3 S2 S1 S0
x19x18x17x16
F0
x15x14x13x12
F1
x11x10x9x8
F1
x7x6x5x4
F1
x3x2x1x0
F0
q4 q3 q2 q1 q0
F2
AUTHEN(i)
RN(i)

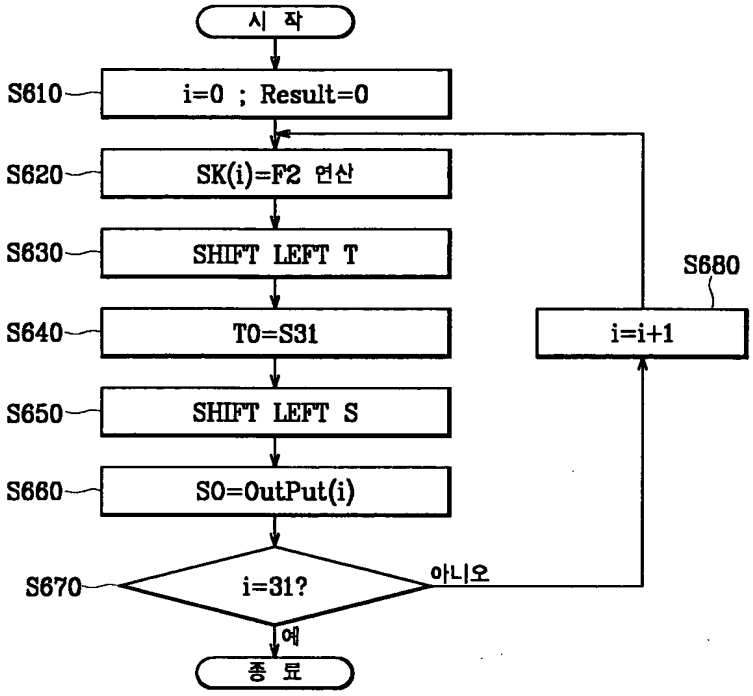
【도 4】


시 작
S410
i=0
S420
F2 연산
S430
SHIFT LEFT T
S440
T0=S31
S450
SHIFT LEFT S
S460
S0=RN(i)⊕AUTHEN(i)⊕F2
S470
i=31?
아니오
예
종 료
S480
i=i+1

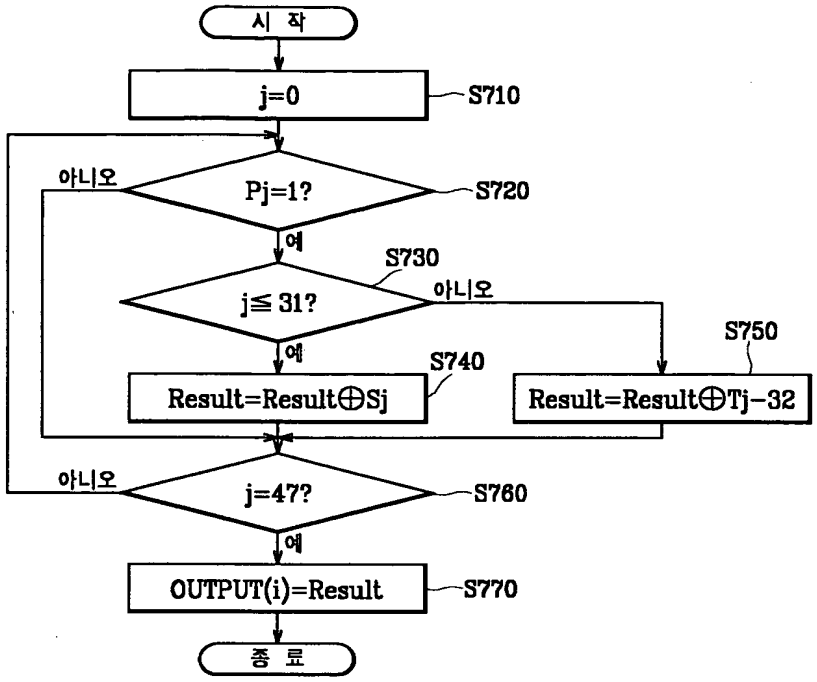
【도 5】


Internal Key P
session key
F2
F1
F1
F1
F0
F0
MSB
LSB
MSB
LSB
시프트 레지스터 T
시프트 레지스터 S
RESULTn
RESULTn-1
REG.(LSB)
Pn
A
0

【도 6】


시 작
S610
i=0 ; Result=0
S620
SK(i)=F2 연산
S630
SHIFT LEFT T
S640
T0=S31
S650
SHIFT LEFT S
S660
S0=OutPut(i)
S670
i=31?
아니오
예
종 료
S680
i=i+1

【도 7】


시 작
j=0
S710
아니오
Pj=1?
S720
예
S730
j≦31?
아니오
S750
예
S740
Result=Result⊕Sj
Result=Result⊕Tj-32
아니오
j=47?
S760
예
OUTPUT(i)=Result
S770
종 료